

## THE TERMINAL MEN

By Willie Schatz June 24, 1990

They first sprang into existence as cartoon characters whose sole purpose was making life miserable for television's "Super Friends." They were the Legion of Doom, and they were led by arch-criminal Lex Luthor.

In the end, of course, even the elite Legion proved no match for the likes of Superman and went the way of most of his enemies -- consigned to cartoon oblivion.

But the Legion of Doom was reincarnated in a different form in the early 1980s by a group of adventurers poised on the edge of the electronic age. They called themselves hackers, and their quarry was not a visitor from another planet. The target for "Phiber Optik," "Acid Phreak" and "Knight Lightning," as some members of the Legion called themselves, was -- and still is -- the computer.

The telephone networks linking corporate and government computer systems were their maze. The passwords and security screens that protected networks from outsiders' access were obstacles to outwit. They schemed to get inside these systems and browse through information files at will.

It was a game, hacker versus hacker, played in unfettered spirit of discovery.

"Hackers will do just about anything that doesn't involve crashing {bringing down} a system," said a New York City Legion member who goes by the computer name of "Acid Phreak," but who would not further identify himself. "That's the only taboo. We don't sell military secrets. We're just out to learn. We transfer data about records that we find in systems. But we draw the line on how we use that data. We use it to play around, not abuse it."

And then, without much warning, it wasn't just a game anymore.

For a diverse group of men from New York City, Middletown, Md., and elsewhere, the change announced itself in the past few months through a series of knocks on the door by investigators bearing warrants. In raids that followed a two-year, nationwide investigation of potential computer fraud, Secret Service agents seized 42 computers, 23,000 computer disks and other items from hackers, including Acid Phreak and Phiber Optik. The equipment will not be returned to its owners until the service finishes examining it as evidence for possible criminal violations.

So far, the Secret Service sweep -- called Operation Sun Devil -- has produced only two arrests.

Other investigations linked to the Secret Service campaign have resulted in several indictments of hackers, some of whom are alleged to be members of the Legion of Doom. Those indicted have been charged with

violations such as using a computer without authorization, interstate transportation of the private information that was in the computer and fraudulently sending unauthorized information across state lines.

"We're authorized to enforce the computer fraud act, and we're doing it to the best of our ability," said Garry Jenkins, assistant director of investigations for the Secret Service. "We're not interested in cases that are at the lowest threshold of violating the law," such as accessing a government computer without authorization, he said. "They have to be major criminal violators before we get involved."

The law enforcer's view of the hacker contrasts sharply with the more benign view of just a few years ago, views that the hacker community still holds today.

"The government's busting kids just for being curious," said the hacker Acid Phreak. "Just because they're in {the system}, they {authorities} automatically assume they're criminals. The government and some companies are getting free lessons in computer security, but they're prosecuting us like we're criminals. It's like hacking's the worst thing since communism. Meanwhile, there are real {computer} criminals out there making real money."

Curious kids or criminals? That the question even is being asked about Legion of Doom members and others shows the dimension of change that has taken place.

When Steven Levy wrote his 1984 book, "Hackers: Heroes of the Computer Revolution," he said: "Hackers are computer programmers and designers who regard computing as the most important thing in the world. Beneath their often unimposing exteriors, they were adventurers, visionaries, risk-takers, artists ... and the ones who most clearly saw why the computer was a truly revolutionary tool."

Among them flows "a common philosophy which seemed tied to the elegantly flowing logic of the computer itself. It was a philosophy of sharing, openness, decentralization and getting your hands on the machine at any cost -- to improve the machines, and to improve the world. ..."

"It's okay to do anything in the name of learning as long as you don't cause harm," a veteran hacker said. "You have the right to access any information that can be accessed {through your technique.} We also feel if they're not smart enough to stop us, we have the right to keep doing anything. That may be technical arrogance, but it's always there."

And there were results from the concentration of all this intellectual energy.

Hacking helped energize both the personal computer industry and the software industry. Steve Jobs and Steve Wozniak, whose creation of the Apple computer made the machine accessible to average people, gained most of their knowledge from hacking. The same holds true for Bill Gates, whose fascination with software eventually led to the creation of Microsoft Corp., now the world's leading producer of operating programs for IBM personal computers.

But with the increasing dependence of business and society upon electronic networks, the incursions of hackers became less and less tolerable.

As early as 1984, a report by the House Judiciary Committee called attention to the "activities of so-called 'hackers,' who have been able to access both private and public computer systems, sometimes with potentially serious results."

- The report also quoted Wilbur Miller, then president of Drake University, who told the committee that there has been a tendency on the part of the public to view such violations as "intellectual pranksterism."
- "This is simply not the case," Miller added. "The ubiquity of computers in virtually every dimension of our everyday lives underlines this point and dictates our concern."
- Congress responded by passing the Counterfeit Access Device and Computer Fraud and Abuse Act, which provided penalties of as much as three months in jail for unauthorized access to computers. A 1986 revision established criminal penalties for six additional types of unauthorized computer access, including entering government computers.
- The legislation, while not halting hacking, apparently has curbed it severely.
- The law authorized the Secret Service to investigate offenses, and the agency has responded in ways that have spawned something of a backlash among computer users.
- Mitchell Kapor, the inventor of Lotus 1-2-3, the world's most popular financial software package, is expected to announce next month the formation of a coalition that will establish a hackers' legal defense fund, lobby Congress to change the 1984 law and help fight what Kapor said had the potential to be a "witch hunt."

## Birth of the Legion

- None of this was an issue when the creator of the Legion of Doom took as his model Lex Luthor and the cartoon Legion. The computer group was loosely based on the television characters, who had names such as Black Manta and Bizarro.
- "The name {Legion of Doom} has nothing to do with the group's intentions," said an 18-year-old New Yorker whose computer name is Phiber Optik. The name is a cartoon spoof, he said.
- "But it is a name that demands respect," he said. "Its purpose was to get the best minds of the time together and have them communicate with each other. The name doesn't demand any respect now, though. It accomplished much more a few years ago."
- And the group, which he said never had more than 15 to 20 members, apparently has become much less particular about the quality of those members.

THE TEDMINIAL MENT TILL WILLIAM D. ..

"Now it's almost like if you say you're in, you are," said another Legion member, a computer consultant whose equipment was seized by the Secret Service as part of the Sun Devil investigation. "We don't have the same standards.

"And I think a lot of our goals have changed," he added. "I know I won't be able to hack the way I used to."

Despite the absence of their hardware and software, however, the two are far better off than one of their alleged Legion colleagues.

## A Hacker's Obsession

Leonard Rose Jr., a 31-year-old computer consultant and hacker from Middletown, Md., whose computer name is "Terminus," had his house searched Feb. 2 as part of Operation Sun Devil. According to Rose, it required half a moving truck and a 35-page inventory to account for the possessions removed by the agency. He also says the seizure has left him unable to operate his consulting company, Netsys Inc.

As a result of the search, Rose was indicted May 15 in Baltimore on five counts of computer fraud, including electronically transmitting a computer program that was the property of American Telephone & Telegraph Co., charges Rose has denied. According to the indictment, Rose was "associated" with the Legion.

Rose began his lifelong fascination with electronics when he was 5 years old. His father, an engineer who tested solid-fuel rocket engines for Morton Thiokol Corp., gave Rose old junk radios. Rose would take them to the basement of the family's Elkton, Md., house and disassemble them. Then he started building radios from scratch.

After a six-year Army stint spent mostly in Korea, Rose moved to New York's suburbs and began designing computer axial tomography (CAT) scanners and magnetic resonance image (MRI) machines for major medical technological companies. While performing those tasks, he established a bulletin board called "APPLENET" that eventually attracted hundreds of subscribers.

"I was a hacker in the original sense -- someone who loves computers and can learn as much as can be learned about a computer," Rose said in an interview.

"I was obsessed. Hacking gave me the edge on my peers and co-workers. The higher the technology I worked on, the better my career would be. Other people didn't stand a chance when they were competing with me. That was my goal and that's what happened. I think it was a psychological carryover from my days in the cellar. But I never let it take over my life. I didn't lose perspective."

His obsession had intensified by 1985, when he moved to Baltimore to take a job with a local medical technology company and he and his Korean-born wife had their first child. Rose continued to hone his skills through the use of more advanced computer equipment, and that expertise made Netsys successful.

Then the Secret Service came. Since its visit, Rose said, his client base has dwindled to one Baltimore-based accounting firm.

The Battle Continues ...

For its part, the Secret Service says it isn't targeting any particular group of hackers.

"We don't really know who belongs to the Legion of Doom," said Dale Boll, assistant special agent in charge of the Secret Service's fraud division. "We've never given them much real credence. ... They haven't been a predisposed target. We focus on individuals committing serious offenses."

"We are not in the business of slowing down technological innovation or stopping the Lewis and Clarks of the 21st century," said Earl Devaney, special agent in charge of the fraud division. "We're only looking for folks committing federal crimes and doing malicious damage."

"We think the deterrent effect of Operation Sun Devil has been very beneficial," he added. "A lot of hackers get lulled into a sense of anonymity behind their computers. There's a psychological sense they won't get caught. But now they know they will."

That thought may slow them, but it apparently will not stop them.

"After all this stuff, we know what not to do next time," Phiber Optik said. "And there will always be a next time."

